Netoscope project:
control of malicious activity in .RU

p.khramtsov@msk-ix.ru
Simple idea:

Nobody uses the same accounts for malicious and respectable activity.

It means -
If you find a malicious activity on one domain you can find it on the other domains of the same account with a high probability.

Registry has got all information about all domains but Registry has not cyber-security skills.
Netoscope project: cooperation of professionals

Координационный центр национального домена Сети Интернет

Роскомнадзор
Group-IB
Лаборатория Касперского
Mail.ru

ФинОфис
Ростелеком
Технический Центр Интернет
Яндекс
БИЗон
Netoscope project: Interaction scheme

Step 1: Malicious domain name

Step 2: All domains on the account

Step 3: All domains from previous step after check

Step 4: Accumulates information into DB

Expert* is a participant of the project
Next actions:

1. Notice to Registrar
   - Registrant personal data check
   - Delegation switch off

2. Notice to Competent Organization
   - Notice to Registrar
   - Registrant personal data check
   - Delegation switch off

3. Project DB
   - Project participant DB
   - Internet end user

Direct actions

Indirect influence
Netoscope project: Statistics

Growth of the Netoscope database (by years)*

- Domain names with verified malicious activity, mln
- Domain names suspected in malicious activity, mln
- Total number of domain names in the Netoscope database, mln

* Second-level, third-level and lower .RU, .РФ and .SU domain names are taken into account
Netoscope project: Statistics

Malicious domain names by categories (by months) *

* Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account. One domain name can be associated with different types of malicious activity at once.
Netoscope project: Statistics

Total number of domains in database (MALWARE)
(by months*)

Number of domain names (malware) - Blue
% of all malicious domains - Red

* Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account.
Netoscope project: Statistics

Total number of domain entries in database (PHISHING) (by months*)

- Number of domain names ( phishing )
- % of all malicious domains

* Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account.
Netoscope project: Statistics

Malicious domain names in Runet by categories
(January 2017)*

* Second-level, third-level and lower .RU, .РФ and .SU malicious domain names are taken into account. One domain name can be associated with different types of malicious activity at once.
Netoscope project: Delegation was switched off

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of requests from CO to Registrars</th>
<th>Delegation was switched off</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>194</td>
<td>59</td>
</tr>
</tbody>
</table>

- Fraud (40%)
- Phishing (37%)
- Malware (10%)
- Spam (10%)
Resume:

1. Cooperation is useful for an indirect way of an influence on the malicious activity
2. It is not easy to switch off delegation if personal data of registrant are correct. We need decision of the Court.
3. Direct international cooperation is possible (we blocked 300 000 in November of 2016 by the request of Shadowserver.org) but it is very strong remedy and can not be used frequently.